A supplier invoice email looks suspicious: checks for venue staff

An unexpected payment request should follow the venue's verification process before anyone changes bank details or sends money.

Practical staff guidance; adapt the suggested workflow to your venue and current procedures.

Notice a change in the request

A message may copy a familiar supplier's style while asking for a new account, urgent payment or a login through a link. Treat changes in payment instructions as a reason to verify the request. A familiar display name or a convincing logo provides limited reassurance on its own. Follow the same process even during a busy service.

Verify through a trusted route

Use contact details already held in the approved supplier record or another independently verified channel. Ask the authorised person to confirm the change. Avoid using the suspicious message's contact information as the sole verification route. Keep financial approval separate from the pressure created by the email's deadline.

Report promptly if something happened

If a colleague clicked, entered information or made a payment, report through the business's incident process promptly and accurately. Give the time, system and action taken. Follow the authorised response instructions so the team can contain the issue and seek the relevant support. NCSC guidance provides practical information about recognising attacks and responding to suspicious messages.

Turn the example into a staff briefing

Use a fictional invoice message with an invented supplier and bank details removed. Ask staff to identify the unusual request and explain the next action. Record the reporting contact where employees can find it. A clear process makes it easier for a colleague to raise a concern early, including after an honest mistake.

Worked example

Fictional example: "Harbour Supplies" emails new bank details just before closing. The duty manager holds the payment change and calls the supplier using the number already in the approved records. The team records the outcome through its normal verification process.

Your next steps

- Pause the requested change.
- Keep the message available for the authorised team.
- Verify using an independent trusted route.
- Use the normal payment approval process.
- Report any interaction promptly.

Verify using a trusted route

An urgent message about changed bank details should trigger the business verification process. Use contact information already held through an approved source, rather than a number or link supplied in the suspicious message. Keep the payment on hold while authorised staff verify the request. Explain how reservations, kitchen and office staff pass a suspicious message to the person responsible without spreading risky attachments.

Record the outcome of the check

Fictional example: a supplier email requests payment to a new account before a delivery. The bookkeeper calls the established contact using the saved number and discovers that no change was requested. The message is reported through the business cyber procedure and any attempted payment is handled promptly by the authorised person. Keep the time, verification route and outcome in the record; avoid recording passwords or full credentials.

What if someone already clicked or paid?

Report immediately through the organisation’s incident process so the right people can act. Fast reporting is more useful than hiding an error. Staff should follow the IT or financial response instructions rather than improvising technical recovery.

A booking amendment arrives with a new payment link

An email using a familiar event organiser’s name asks the venue to pay a revised invoice today. The amount looks right but the account details have changed. What should reception do?

Compare your decision

Leave the link unopened and verify the request through an independently known contact route. Follow the venue’s payment and security reporting procedures. Preserve the message for the responsible team. Replying to the same email would only reach whoever controls that mailbox.

Practise finding the trusted contact without opening the attachment. Record who confirmed the change and how, using the approved finance process.

Sources and editorial basis

- NCSC — Spotting cyber attacks

Guidance checked on 19 October 2026. Examples and worksheets are original suggested workflows; adapt them to your operation.

Use this on shift

Resource page and fillable working record · Read the online guide · Course details